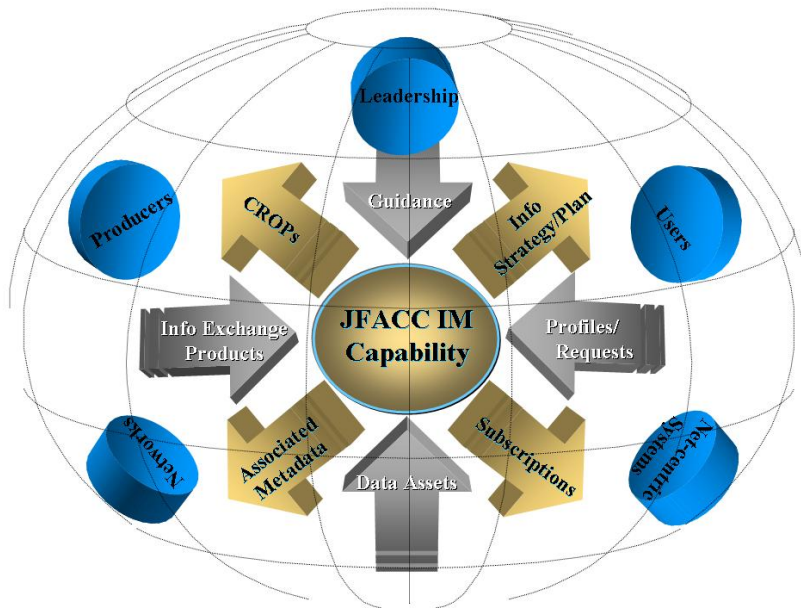


MTR 06B0000007

MITRE TECHNICAL REPORT

JFACC Information Management (IM) Capability

Operational Concept



January 2006

J. Cook

J. Vittori

Sponsor: AFC2ISRC/CTA
Dept. No.: D440

Contract No.: FA8721-06-C-0001
Project No.: 0306698A-CX

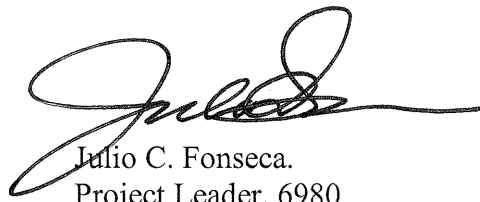
The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

©2006 The MITRE Corporation. All Rights Reserved.

MITRE
Langley Site Operations
Hampton, Virginia

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JAN 2006		2. REPORT TYPE		3. DATES COVERED 00-01-2006 to 00-01-2006	
4. TITLE AND SUBTITLE JFACC Information Management (IM) Capability: Operational Concept				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) MITRE Corporation, Langley Site Operations, Hampton, VA, 23666				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 52	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Approval Page

A handwritten signature in black ink, appearing to read 'Julio C. Fonseca', with a long horizontal flourish extending to the right.

Julio C. Fonseca.
Project Leader, 6980
Air Force Integrated C2

Abstract

This paper details an operational concept calling for an Information Management (IM) capability to support a Joint Force Air and Space Component Commander (JFACC) and an Air and Space Component in 2010. It proposes the establishment of a Community of Interest (COI) construct, a JFACC IM organization, and the supporting operational processes.

Throughout the Department of Defense (DoD) there are numerous ongoing efforts supporting the goal of “net-centricity”. Most of the impetus is system-oriented or reflects a system-centric approach. The concept described in this paper focuses on the operational aspects, i.e., business processes supporting the JFACC that will take full advantage of the net-centric environment in 2010. The proposed concept presents an approach to make data visible, accessible, understandable, and trustable. It allows information managers to reach across traditionally stove-piped organizations’ processes and applications to “meld” the information within a net-centric environment and allow users to seek and use the information they need across the battlespace.

The first chapter defines the problem space for the MITRE architecture team of Jay Vittori and Jeff Cook. Chapter 2 details their analysis process and how they framed their IM vision for 2010. Chapter 3 highlights the major precepts of that vision, the JFACC Information Management Capability Concept. Chapter 4 contains the specific processes associated with the concept, i.e., processes to: provide information management/net-centricity governance; manage information/net-centric data accessibility; manage the JFACC’s net-centric data; build and monitor net-centric pictures; and manage information assurance/network defense operations within a net-centric environment. The intent of this paper is not to dismiss existing or evolving IM- or Net-Centric undertakings; rather, it should enhance those efforts by providing an operational perspective on how to manage data and information within a Joint force environment.

Table of Contents

1	The Challenge	1-1
2	Forming the Vision	2-1
3	IM Capability Concept Precepts	3-1
3.1	Push and Pull Smartly	3-1
3.2	Make Decision Quality Information (DQI) a Top Priority	3-1
3.3	Break it Down to Build It Right	3-2
3.4	Exploit Data Assets to Paint the Right Picture	3-3
3.5	Exploit Shared Space through an OASIS	3-6
3.6	Understand that Point-to-Point is not Pointless	3-7
3.7	Establish a JFACC Component Community of Interest	3-8
3.8	Maintain a Robust JFACC IM Organization	3-9
3.8.1	Information Management Officer (IMO) - Air	3-10
3.8.2	Information Management Board (IMB) - Air	3-11
3.8.3	Information Management Cell (IMC) -Air	3-11
3.9	Make Security Paramount	3-11
3.10	The JFACC IM Capability Concept	3-12
4	Key Operational Processes Defined	4-1
4.1	Management – Provide Information Management/Net-Centricity Governance	4-2
4.1.1	Provide Component Net-centric/Info Management Organization	4-2
4.1.2	Establish Component Commander’s Information Requirements (CCIRs)	4-4
4.1.3	Establish the JFACC IM Strategy and Plan	4-5
4.1.4	Establish Component Data Standards, Metrics, and Incentives	4-6
4.1.5	Establish User Profile Standards	4-6
4.2	Manage Information/Net-centric Data Accessibility	4-6
4.2.1	Provide Data Access Services	4-7
4.2.2	Process Component Information Requirements	4-7
4.2.3	Manage Shared Space/Repositories	4-8

4.3	Treatment – Manage Organizational Net-Centric Data	4-8
4.3.1	Define Component Ontologies	4-8
4.3.2	Identify Data Asset Requirements	4-9
4.3.3	Associate Metadata with Data Asset	4-10
4.3.4	Post Asset to Shared Space	4-11
4.3.5	Register Metadata	4-11
4.3.6	Manage the Metadata Catalog	4-11
4.4	Manage Net-centric Pictures and Products	4-11
4.4.1	Process Component CROP Development Request	4-11
4.4.2	Develop Component CROP(s)	4-12
4.4.3	Release and Monitor Component CROP(s)	4-13
4.5	Protection – Manage Component Information Assurance/Network Defense Operations	4-13
4.5.1	Manage Component INFOCON	4-13
4.5.2	Support Information Assurance Vulnerability Alert (IAVA) Program	4-14
4.5.3	Monitor Component Communications Links and Networks	4-14
4.5.4	Manage Network Attack Impact Assessment	4-14
5	Summary	5-1
	References	R-1
	Glossary	G-1
	Acronyms	G-4

List of Figures

Figure 2-1. The Push Paradigm	2-1
Figure 3-1: Data Asset Example	3-3
Figure 3-2: Data Asset, IEP, CROP Examples	3-4
Figure 3-3: Data Asset, IEP, CROP Examples	3-5
Figure 3-4: CROP Interrelationship to the COP	3-6
Figure 3-5: OASIS Concept.....	3-7
Figure 3-6: COI Construct	3-9
Figure 3-7: IM Organizational Construct	3-10
Figure 3-8: High-level Operational Concept Graphic	3-12
Figure 4-1: Key Ops Processes	4-1

1 The Challenge

In 2003, Air Force Command and Control & Intelligence, Surveillance and Reconnaissance Center (AFC2ISRC) tasked its MITRE architecture team to define architecturally the Command and Control Constellation (C2C) as rationalized then and as projected for 2012. In its baseline form, the C2C was basically a loose confederation of key Air Force and Joint command and control (C2) and intelligence, surveillance and reconnaissance (ISR) operational nodes. The C2C represented a family of systems (FoS) that would operate synergistically to interface with other national, interagency, multinational (alliance/coalition), Service, and functional nodes. Presumably, the degree of integration within the FoS and the synergistic effect rendered would increase over time.

The progression was predicated upon several factors, most of which are fairly obvious, namely advancements in technology, forecasted and funded systems upgrades, and projected new system starts. Perhaps less apparent, were the theoretical aspects relating to operational or business process changes. The Air Force was promoting three major process shifts: Effects-based Operations, Predictive Battlespace Awareness, and Net-Centric Operations. Effects-based Operations (EBO) would invoke a paradigm shift from target-centric operations to those driven by desired effects. This would alter key operational planning, execution and assessment processes. Predictive Battlespace Awareness (PBA) was less clearly defined. At the time, PBA instantiations abounded and continued to evolve. For the tasking, the architects incorporated the predictive aspects of PBA, i.e., those processes used by C2 experts to analyze and understand adversaries and predict their reactions, strategies, objectives, etc. The third shift, Net-Centric Operations was considered a “hot button” topic. Most understood the relative importance net-centricity. Very few at the time knew how to achieve it, especially in regard to air and space operations. Frankly, the MITRE architecture team members Jay Vittori and Jeff Cook who were tasked to architect this aspect did not know either.

The reader is not expected to see everything on this graphic. Its inclusion provides a vivid example of the today's "sausage making" process for picture development. Massive numbers of information exchanges feed into operational activities (yellow rectangles). The information is pushed to the consumer. Each arrow coming in from the right of an activity represents an information product such as a message, report, order, etc. Those executing the receiving activity take what they need from the information products. They build other information products that support other activities in the process. These products are also filtered out until final products, or in this example, pictures are produced.

This Push Paradigm and its associated packaging concept are problematic. First, the consumer often receives far more information than required. For example, a flying unit trying to find its tasking for the following day will have to receive an entire Air Tasking Order (ATO). That means the unit will typically use 8-10 pages of a 2000 page document. The unused portions were pushed through the system regardless of the recipient's needs. This causes an unnecessary burden on transmission systems and associated connections, the "pipes". It is also an encumbrance for the consumer who must wade through those 2000 pages to find the "nuggets" of required information. For operational pictures, the problem is exacerbated. There are far more products to examine and exploit. Information melding is often manual, that is, it requires a great deal of human interface to decipher data and information, glean the requisite information, build the desired representation, and disseminate it to the proper users. In summary, today's Push Paradigm pumps a great deal of information through our communications pipes to support a desired product when only portions of that information are actually required. This inefficient process impacts communications systems, information managers, and most importantly, information consumers.

The *Air Force Transformation Flight Plan*¹ affirmed many of the obstacles affecting information management and clearly defined the problem space for the team:

- Despite significant gains in information superiority capabilities over the past decade or so, there are still many obstacles to achieving the full potential of information superiority under many circumstances today.
- Battlespace awareness information is often reactive in nature and rapidly loses relevance.
- It is still very difficult to integrate rapidly expanding data streams from multiple sources in a timely manner.

¹ The *Transformation Flight Plan* used for the initial development was published in 2003 and subsequently revised in 2004. The items listed reflect the updated text.

- The military still cannot assess, plan, and direct air and space operations from anywhere or from multiple locations in near real-time
- The Air Force still needs to evaluate its current systems and determine what they can contribute to its capabilities and what tools are necessary to transform those systems from a collection of platforms into a networked system that is greater than the sum of its individual parts.
- The Air Force lacks a scalable C4ISR system that can support operations across the spectrum of conflict.

The team understood the problem space. They turned their attention to the future, particularly 2012, the year selected for the C2C To-Be architecture. Once again, they began with research, this time opting for vision statements, strategies, technology forecasts, lessons learned, and future concept documents. Of those, two key references provided the basis for their information management concept.

The *Air Force Information Strategy* was published in August 2002. Its signatories, the former Secretary of the Air Force, Dr. James G. Roche, and former CSAF, Gen. John P. Jumper, state the strategy

Captures our vision for managing and leveraging information to enhance our Air Force. It describes the information world as it will be: a world where sensors provide instantaneous information to effect decisions...a world where we take advantage of the best practices American industry can provide...a world where our information is totally protected from attack and compromise.²

The document goes on to detail nine goals for information management. Of those, the team focused on the following five for their architecture:³

- Despite significant gains in information superiority capabilities over the past decade or so, there are still many obstacles to achieving the full potential of information superiority under many circumstances today.
- Battlespace awareness information is often reactive in nature and rapidly loses relevance.

² *Air Force Information Strategy*, August 2002, Foreword

³ *Ibid*; The C2C architecture represents a Joint perspective; the other four goals were AF-specific.

- It is still very difficult to integrate rapidly expanding data streams from multiple sources in a timely manner.
- The military still cannot assess, plan, and direct air and space operations from anywhere or from multiple locations in near real-time
- The Air Force still needs to evaluate its current systems and determine what they can contribute to its capabilities and what tools are necessary to transform those systems from a collection of platforms into a networked system that is greater than the sum of its individual parts.
- The Air Force lacks a scalable C4ISR system that can support operations across the spectrum of conflict.

The second key document was the *DoD Net-Centric Data Strategy* published on 9 May 2003. The former DoD Chief Information Officer, John P. Stenbit, states this document “outlines the vision for managing data in this net-centric environment”.⁴ This strategy also provided the following key goals for the architecture and provided the framework for the information management portion of the C2C activity model.

- Make Data Visible
- Make Data Accessible
- Institutionalize Data Management
- Enable Data to be Understandable
- Enable Data to be Trusted
- Support Data Interoperability
- Be Responsive to User Needs

Armed with the vision of net-centricity the team began strategy development, i.e., how should current operational processes change to make the vision a reality by 2010. Utilizing the baseline architecture products and the aforementioned goals, the team formulated nine key precepts that would allow them to forecast JFACC information management processes.

⁴ *Department of Defense Net-centric Data Strategy*, 9 May 2003, Foreword

3 IM Capability Concept Precepts

3.1 Push and Pull Smartly

The earlier discussion on the Push Paradigm demonstrated the dilemmas caused by improperly pushing data and information. Pushing can be the right approach if it is done smartly and in tandem with Smart Pull. Smart Push presumes the sender determines which information is transmitted. The sender publishes to the net. A smart “pusher” only publishes data/information that presumably interests a consumer. On the other hand, Smart Pull is a demand-centric approach whereby the receiver determines what enters the net. If no consumer demand exists, the product is not published. There are benefits and problems associated with both approaches. Smart Push provides information readily that perhaps the consumer did not realize was needed or available. It presumes the user may not understand all of his/her information requirements or the availability of information. The downside to Smart Push is that assumptions about product demand may be inaccurate, thus burdening the net with superfluous information. Smart Pull allows the consumer to dictate the data/information content on the net. On the surface, this appears to be a much more effective approach. Unfortunately, it relies on two critical factors, i.e., the consumer knows what he/she wants and what could be available. Neither may always be the case.

Debates about the primacy of a smart push versus a smart pull are unnecessary. It is essential for both aspects to work in concert. If we have educated consumers that explicitly state demands, we can push more effectively. Likewise, if we have knowledgeable producers publicizing data/information availability, we can pull with prowess.

Bandwidth is and will remain a critical factor. Far too often the networking solution is focused on the size of the “pipes”. Size does matter, but should not be the only or even the foremost area of concern for communicators. Today’s bandwidth overloads are driven by inefficiencies wider ranging than capacity. Most problems relate directly to poor, push/pull techniques. The key to alleviating bandwidth problems is regulation or control. It’s not only what is transmitted, it is also when it is sent. A gigabit per second download is a burden, but not debilitating if it occurs at the right times. It is comparable to water at a dam; we need to regulate the release to alleviate back-up yet not cause flooding. In the future, Smart Push/Pull will create greater efficiencies within the net-centric environment.

3.2 Make Decision Quality Information (DQI) a Top Priority

For an organization to function well, the leaders need to make the “right” decisions. While it is correct to assume perfect information does not guarantee the right choices, it is fair to presume decision makers manage better with better information. Generally, commanders are entrusted to make key decisions, many of which will determine the efficacy of their organizations. Future information management processes should provide commanders the “right” input to make the “right” choices. That “right” input is called Decision Quality Information (DQI).

At the top of the C2 hierarchy are the key decisions made by leaders. An organization's top priorities are to identify those decisions and then to establish the information needs or requirements to support them. Thus, DQI belongs at the top of the information "food chain" and it drives the decision support processes and systems.

Not all information is DQI. Additionally, not all information is useless. There will likely be a need for non-DQI in an organization and processes and systems should support its production. It is essential to avoid the useless or superfluous data/information. Future information processes will cull the right data and information, especially for decision makers. The "nice to have" input is just that unless it bogs down the decision process; it then becomes a distraction. Sometimes, the bottom line should be the only line.

It is unreasonable to assume IM processes will ever make communications processes perfect. It is conceivable they can radically improve them by focusing on DQI and the decisions it supports.

3.3 Break it Down to Build It Right

As presented earlier, Smart Push/Pull can help with bandwidth overload. Another way is data culling or parsing. Instead of passing an entire report, document, briefing etc, send only what the consumer wants. For example, viewers watching the evening news do not know exactly what topics will be covered or when they will occur. To hear news of interest, viewers may be forced to sit through coverage they care little about. They have virtually no influence over product delivery. The newspaper affords readers a little more control. Even though subscribers receive newspaper sections of little or no value, they don't have to peruse them. The friendly internet is an even more efficient news provider. Subscribers don't have anything to throw away. They take what they want from the service.

In the future, data culling or parsing will allow our standard work products to be provided with similar efficiency. Today, the size of an Air Tasking Order (ATO) is relative to the number of missions tasked. It is not uncommon to have a 1000-2000 page order. For years, the ATO was sent out in its entirety to all concerned parties. Each tasked organization had to "frag break" or find and process the applicable information. As discussed earlier, the relevant information may be less than ten pages. The rest of the document is unused. In the future, data culling and subscription applications will allow the organization to receive only the tasking needed or requested.

An operational example of this concept is shown in Figure 3-1. Air refueling (A/R) operations rely on essential data. Among other data assets, A/R operations require an Air Refueling Control Time (ARCT), applicable Airspace Control Measures (ACM), and receiver Take-Off times. Today, the entire ATO, Airspace Control Order (ACO), and Take-off Report are "pushed" to the refueler's ground support unit where the needed information is culled.

In 2010, the air refueler unit asks for (pulls) and receives its required information. The request is established through a user profile and controls are invoked at the information source. The bulky products associated with the required information are not transmitted, thus saving bandwidth.

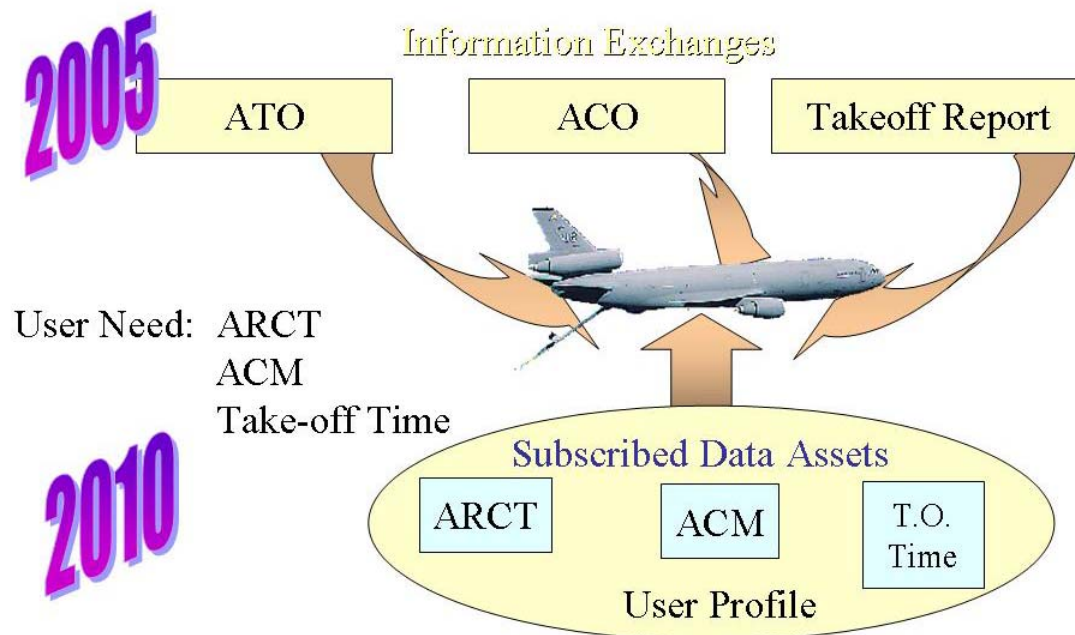


Figure 3-1: Data Asset Example

There is an inherent danger with this methodology. The receiver needs to understand the meaning of these data assets and the context in which they were and can be applied. Metadata, the data about data provides much of this context. Faulty or inadequate metadata may lead to the improper use of a data asset. Additionally, there are security risks which are examined in a later section. Regardless, proper application of metadata will allow subscribers to exploit data assets from various sources to develop tailored information products that meet their individual needs. Realistically, they can create their own news, reports, analyses, etc and receive it whenever they choose.

3.4 Exploit Data Assets to Paint the Right Picture

The team understood that by 2010, IM systems could not accommodate the free flow of data and that the operator would probably prefer common aggregations of data and information. The JFACC Information Management Capability Concept provides a hierarchical grouping for these aggregations (Figure 3-2). At the lowest level is the Data Asset, which is any entity composed of data required by a user. A data asset could be a takeoff time, target database,

radar return, image, etc. A data asset may serve as a key element of an Information Exchange Product (IEP).

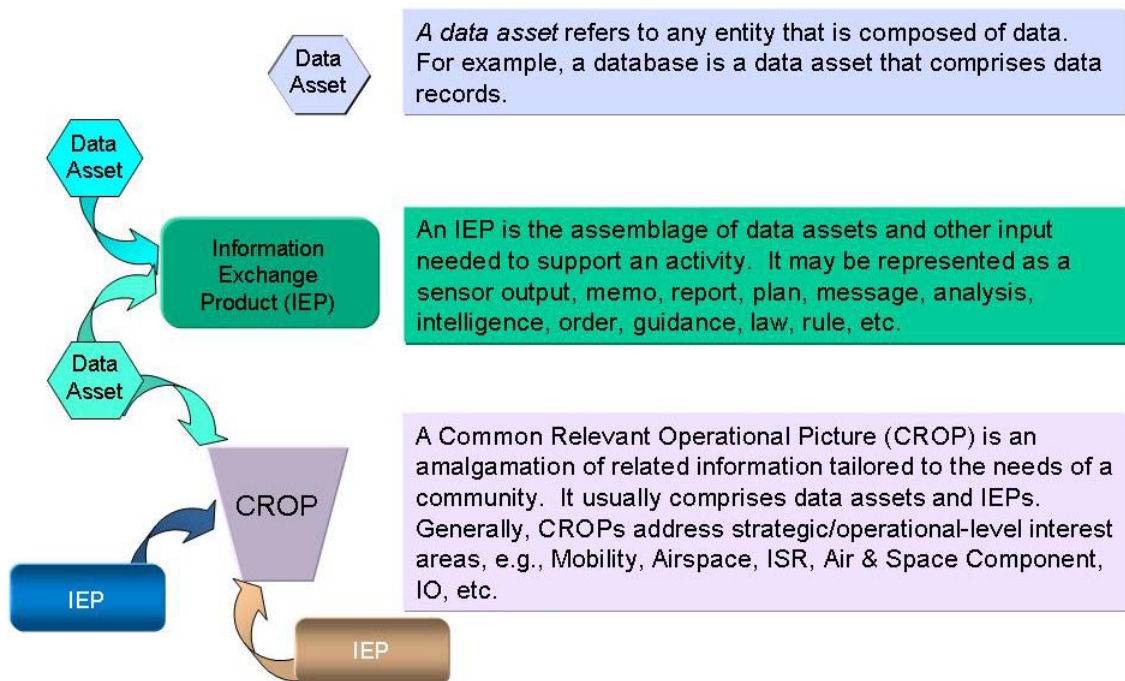


Figure 3-2: Data Asset, IEP, CROP Examples

An IEP is an assemblage of data assets and other input needed to support an activity. It may be represented as a sensor output, memo, report, plan, message, analysis, intelligence, order, guidance, law, rule, etc. The IEP applies context to data assets. The most common IEP today is a message. For example, the ACO comprises of hundreds of data assets supporting airspace management.

Data Assets and IEPs exist today. In the future, the team postulated that communities of interest (COIs) would want relevant data and information amalgamated to meet the needs of that community. The team interpreted this to be a tailored picture that would serve a strategic or operational-level interest (e.g., air mobility, space, air defense, IO, etc.). They called this representation a Common Relevant Operational Picture (CROP).

The team proposed several CROPs to address the JFACC's major interest areas. The data assets within these CROPs may be shared by one another. In fact, the team proposed an Air & Space Component CROP that would glean pertinent data and information from the other CROPs to provide a clear-concise, tailored picture for the JFACC. Figure 3-3 depicts a number of proposed JFACC CROPs. This is a notional representation. Each JFACC should have the authority to direct the assemblage of CROPs to meet operational requirements.

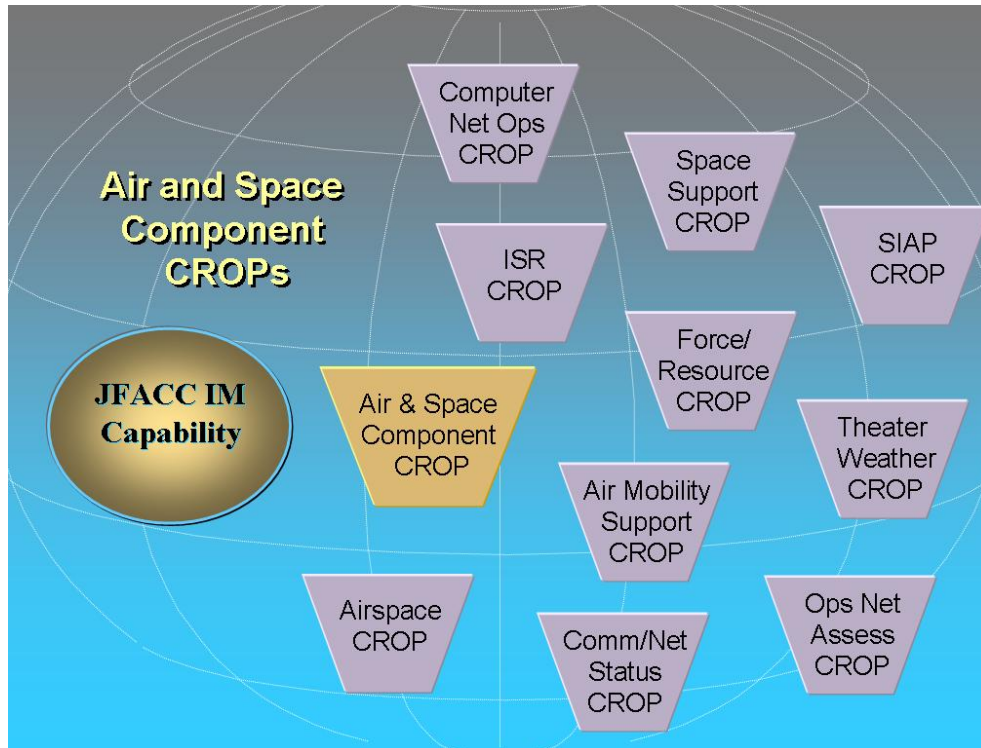


Figure 3-3: Data Asset, IEP, CROP Examples

The team then wanted to show how the Air & Space Component CROP would fit into the “Big Picture”, which they called the Joint Force Commander’s Common Operational Picture (COP). Figure 3-4 depicts the interrelationship between Component and non-Component CROPs. The JFC’s COP is not the totality of the CROPs; rather, it is the aggregation of culled, relevant data assets and IEPs needed to represent the JFC’s operational needs. Once again, this is a notional representation that typifies current Joint Task Force (JTF) relationships.

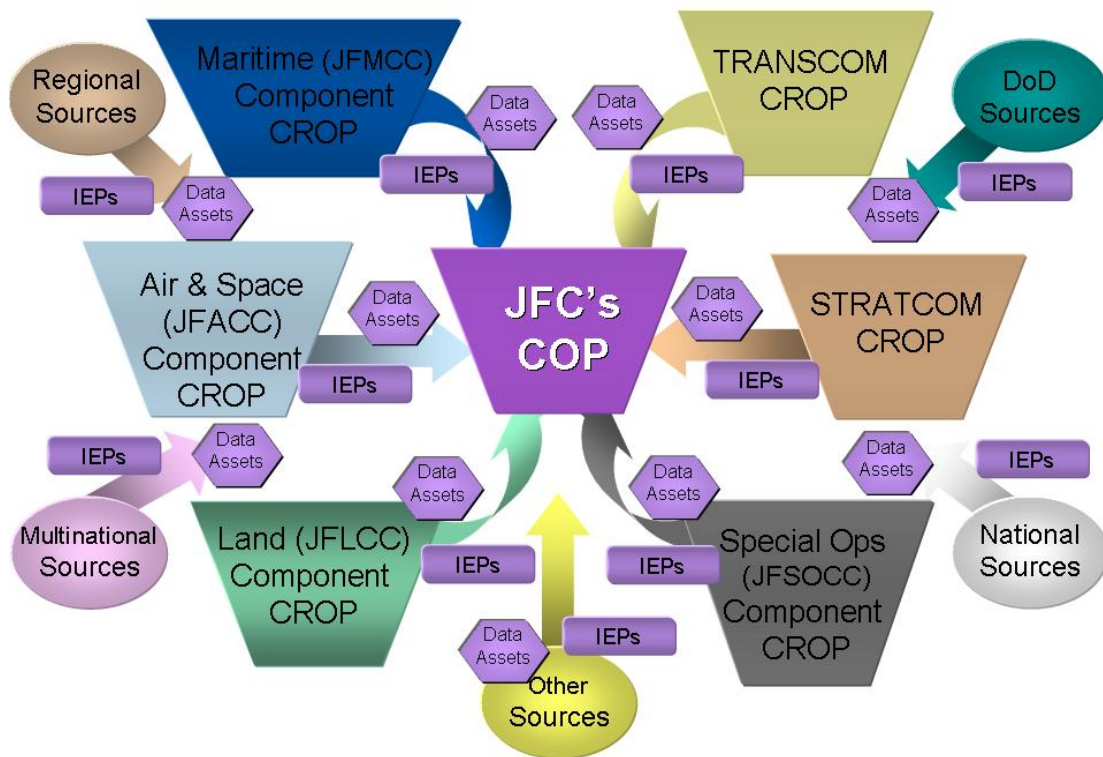


Figure 3-4: CROP Interrelationship to the COP

3.5 Exploit Shared Space through an OASIS

The team coined the term “Operationally Accessible Shared Information Space (OASIS)” to denote the established shared space bounded by specific operational needs that can be focused around missions, functions, threads, etc. An OASIS can be established for missions such as Close Air Support (CAS) or for operational threads that cut across missions, organizations or COIs. Time Sensitive Targeting (TST) is an example of this type of OASIS domain where multiple entities are involved. A single organization should be responsible for the allocation of the shared space and granting access to authorized users. The ownership of the data would remain with the owning organization with the OASIS providing the collaborative environment between all authoritative members.

In the example depicted in Figure 3-5, the JFACC would have overarching responsibility for establishing and maintaining the shared information space and authorizing access/privileges to authorized entities. This is not to say that the control of the data posted to the OASIS is controlled by the JFACC; rather, the JFACC would ensure the operational aspect of the shared information space meets the needs of the authorized entities. All the information required for collaboration and situational awareness is controlled by the authoritative source. The information could be posted within the shared information space or the authoritative source could place a link to the information source. The OASIS is the method for

collaboration within the operational environment, a way to control access, and a way to prevent unneeded traffic from slowing down accessibility.

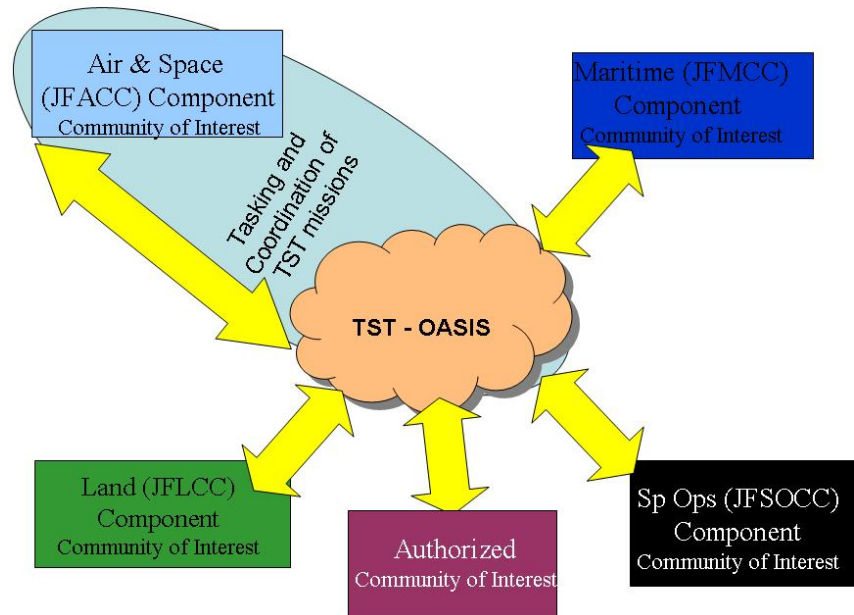


Figure 3-5: OASIS Concept

3.6 Understand that Point-to-Point is not Pointless

Content management was touched upon in several of the preceding sections. If one buys into the precepts this far, one understands the need to regulate the information flow across the net. Perhaps not so apparent is the need to manage the flow outside or beyond the net. Not everything could or should pass through a network. Direct or point-to-point communication outside a network can be a more efficient way to pass information. Some information is too critical for the net, while some is far too mundane. For example, air traffic controllers shouldn't type in landing vectors for approaching aircraft. Also, the net should not host lunch plans, discussions on the weather, or plans for the weekend. Allowing information flow outside the network eases congestion on the net, but may impact overall bandwidth usage.

Connectivity issues may preclude an organization from fully exploiting a network. For various reasons, some key JFACC nodes may not be net-ready. This could be due to technology, i.e., the capability does not exist. It may be attributed to cost, i.e., the USAF is not willing or able to pay for the capability. Lastly, it may be a matter of preference, i.e., there is no need to connect to a network. Some nodes may be net-ready, but the links are not reliable. Cellular phone users ten years ago and those currently coping with wireless LANs and WANs understand these limitations. Link redundancy or the ability to provide a

communications back-up is rationale to maintain at least a modicum of point-to-point connectivity. Not many organizations have removed their hard-line telecommunications capability to rely solely on cellular transmissions. Even with sophisticated hard-wired networks, users still experience the occasional “network down” dilemma. One could either ride it out or seek other methods for communications. As operators are able to trust their links more, the less concerned they may be about back-ups. In the meantime, they should keep their options open.

3.7 Establish a JFACC Component Community of Interest

Since the team began work with this project, the Community of Interest (COI) concept has evolved a great deal. The definition has been relatively stable, but the application has expanded. According to the *Air Force Information and Data Management Strategy Policy*, a COI is “A collaborative group of people who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared definitions for the information they exchange...COIs always contain both information producers and consumers.”⁵ This pretty much echoes the verbiage in the *DOD Net-Centric Data Strategy* published the year prior. No formal COIs were established at the time.

The team saw the benefit of a COI to the JFACC and the Air & Space Component. The *DOD Net-Centric Data Strategy* only called for a DoD COI. The team wanted extend that community out to the JFACC. They developed the COI arrangement depicted in Figure 3-6. The alignment follows functional (e.g., USSTRATCOM, USTRANSCOM) and geographic or regional/theater commands (e.g., EUCOM, PACOM, CENTCOM, etc.) lines. If a Joint Force is established, it will probably operate within a geographic construct and the JFACC will function within that joint force hierarchy. Basically, the COIs at the highest levels would represent the common command entities and the normal chain of command. It is important to note the Air & Space Component COI is a Joint COI, ie., it serves the interests of the entire air & space community supporting the JFACC, not merely those of the Air Force. This community comprises personnel, data/information, and other information assets from functional, Service and multinational (allied/coalition) organizations supporting the JFACC.

⁵ *Air Force Information and Data Management Strategy Policy*, 3 March 2004, pg. 3

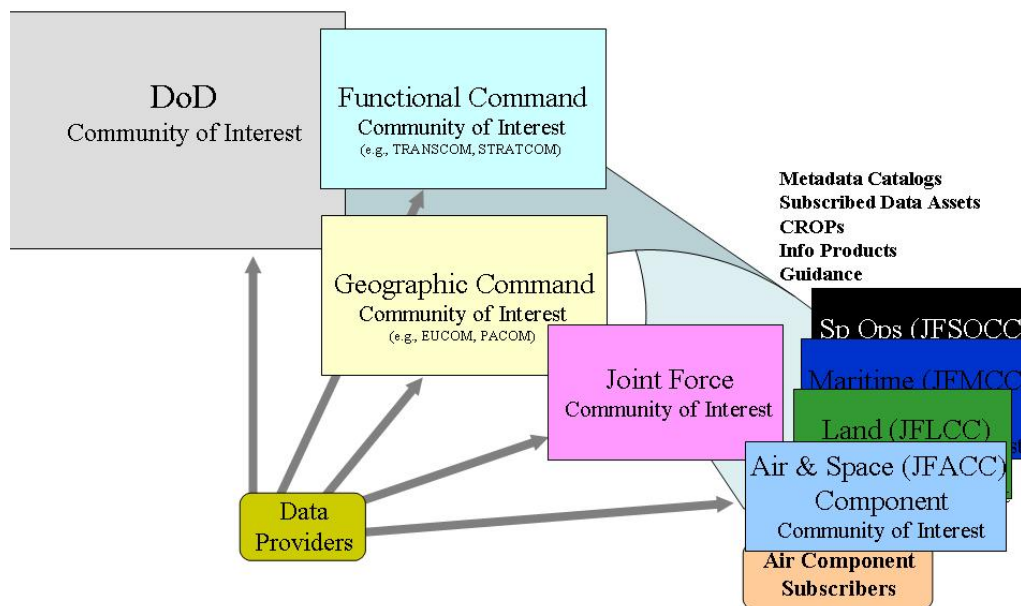


Figure 3-6: COI Construct

This construct does not preclude the implementation of other COIs. Conceivably, a JFACC could form a COI with a mission focus, such as Close Air Support (CAS), one with a system focus, like Theater Battle Management Control System (TBMCS), or another with a node focus, such as Wing Operations Center (WOC). There are many ways to “slice the pie”. It all comes down to operational need. While the team does not prescribe the lower-level COIs, it firmly advocates the establishment of an Air & Space Component COI to serve as an overarching authority and provide clear boundaries for supporting COIs.

3.8 Maintain a Robust JFACC IM Organization

It is evident that the aforementioned precepts can not be carried out by the JFACC alone. The JFACC needs an IM capability to support the Component’s needs. When the team began work on this project, very few Numbered Air Force (NAF) commands had robust IM organizations. In September 2003, the Air Land Sea Application (ALSA) Center published *JTF IM: Multi-Service Tactics, Techniques, and Procedures for Joint Task Force Information Management*. This seminal work provided the basis for a joint IM organizational construct. The team used this design and created the interfaces within the JFACC organization. The relationship is depicted in Figure 3-7.

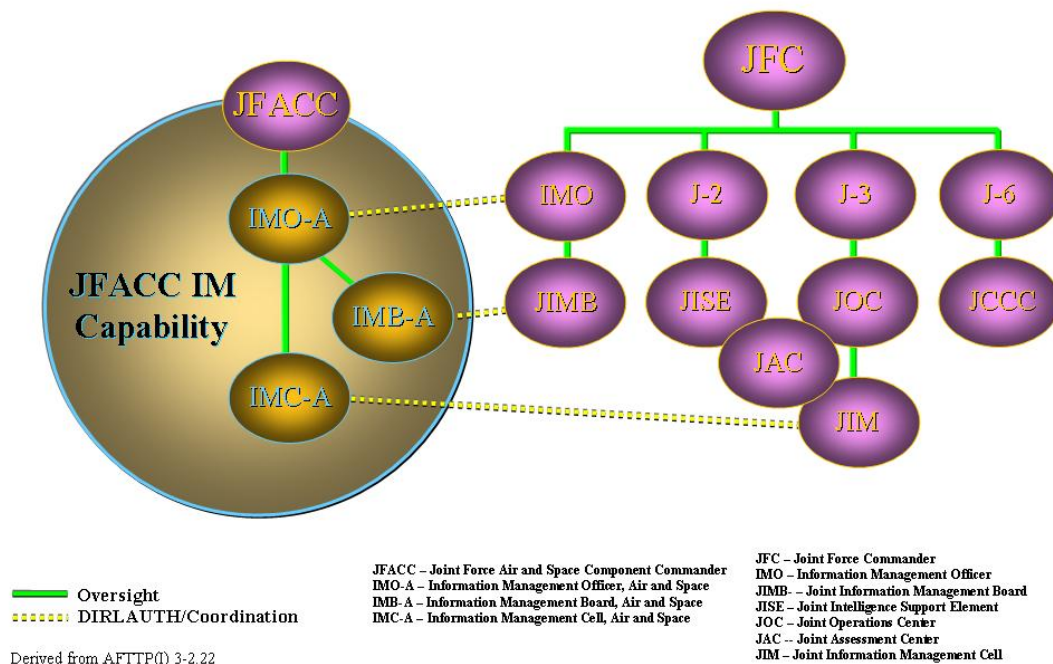


Figure 3-7: IM Organizational Construct

The JFACC IM Capability comprises three main entities: Information Management Officer (IMO), Information Management Board (IMB), and Information Management Cell (IMC). The following subparagraphs describe the attributes of each. Specific responsibilities are detailed in the following chapter. This organizational construct is notional. It is presumed that this capability will reside within the CAOC. It may reside with the AFFOR functionality of the Warfighting Headquarters as long as Joint and multinational representation is provided.

3.8.1 Information Management Officer (IMO) - Air

The IMO-Air is the chief for all JFACC IM activities. The IMO-Air is responsible for coordinating with required external IMOs, IMBs, and other components, as well as publishing the organization's Information Management Plan. The IMO-Air is intimately aware of the commander's information management requirements and possesses the authority to coordinate actions and processes to satisfy essential information needs. Under the supervision of the JFACC's Chief of Staff (CoS), the IMO-Air works closely with higher HQ IMOs to ensure all required reports are up-channeled consistent with the battle rhythm. The IMO-Air serves as the focal point for information management issues with other functional component commander staffs. The IMO-Air also works closely with command administrative staffs and command and control elements (command posts) of all subordinate units in order to define reporting requirements and with Communication Support Team and

communications/computer systems personnel to facilitate necessary information exchanges. The IMOs from the Components or agencies under the JFC will serve on the Joint Information Management Board (JIMB).

3.8.2 Information Management Board (IMB) - Air

The IMB-Air is chaired by the IMO-Air and will operate under the supervision of the JFACC, or other appropriate staff directorate, as determined by the JFACC. The board should comprise representatives from each CAOC division and liason function. The IMB-Air is used to actively resolve all internal, cross-functional, and JIMB-directed information management issues. It convenes on an as required basis. The IMB-Air is the action arm of the IMO-Air and will serve as the key interface with the other established IMBs to resolve IM related issues.

3.8.3 Information Management Cell (IMC) -Air

The IMC-Air acts as the internal focal point for coordinating IM within the organization. The Superintendent of the IMC-Air works closely with the IMO-Air to ensure JFACC IM policies and procedures are implemented and followed throughout their assigned areas. The IMC-Air is responsible for providing processes and business rules for life-cycle management of information as well as user assistance for common software applications. The IMC-Air provides oversight and training to workcenter managers.

3.9 Make Security Paramount

Network security will remain a high priority. Most understand the common threats such as viruses, Trojan horses, worms, etc. The DoD invests a great deal to protect its networks from the gamut of threats ranging from the kid down the street to the spy halfway around the world. The free flow of and accessibility to information throughout the globe is a boon to businesses and consumers alike; however, it also poses risks. Personal or business space is sometimes invaded and exploited. Hence, many DoD security processes, tools, and outlays focus primarily on eliminating infiltration. Passwords, firewalls intrusion detection systems, certification authorities/public key infrastructures, etc. within government networks attempt to protect those within from the Huns beyond. What happens if the enemy lies within and the enemy is you? What if you were inadvertently passing secrets, strategies, technologies, etc.? Is the JFACC organization equipped to protect itself from itself?

These are intriguing questions and ones that must be addressed. As mentioned before, data culling or parsing will become common practice in the years to come. Subscribers will request and receive data that they will compile and apply context. Aggregation of this data can become problematic from a security perspective. The individual data elements or assets may not be of concern, but their consolidation may reveal unintended and perhaps, sensitive information. It is reasonable to assume the greater the aggregation of data assets or data sources, the greater the risk of information leaks.

Thus, the future points toward increased risk to DoD information stores. The JFACC IM Capability must learn to pay now rather than later and take the necessary measures to reduce vulnerabilities. The first step is recognition. Organizations must understand their essential elements of information that must be protected. The next step is education. Information providers must be aware of aggregation risks. The third step is prevention. The JFACC will rely heavily on information management personnel and operations specialists to analyze data consolidations to ensure they are safe. Automation will help but will not eliminate these risks. A strong information management capability is essential to information security.

3.10 The JFACC IM Capability Concept

Utilizing the foregoing precepts the team formulated the JFACC IM Capability Concept. Basically, the JFACC establishes an IM organization that directly interfaces with command authorities, information producers and consumers, internally and externally managed networks, and key systems associated with those networks. The IM Capability processes IM guidance, builds and manages user profiles, works information requests, and exploits data assets and information exchange products. Key outputs include the Component's Information Management Strategy and Plan, fulfilled data/information subscriptions, metadata associations, and the JFACC's CROPs. The following chapter will detail the key operational processes executed by the capability.

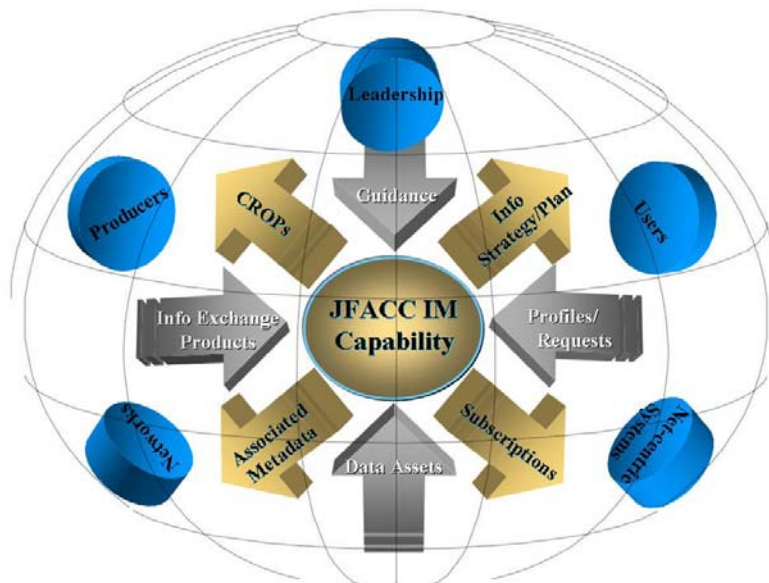


Figure 3-8: High-level Operational Concept Graphic

4 Key Operational Processes Defined

The operational processes discussed in this chapter evolved considerably from the first iteration produced in 2003. Changes occurred as the precepts progressed. Another significant catalyst was architecture. The team developed an initial decomposition of activities and constructed an activity model. The modeling process highlighted the gaps and inconsistencies within the processes. By relating information exchanges to the activities and processes they support, the team was able to better understand how the key operational process domains interrelated. Culminating from several cycles of architecture development and concept refinement, the team established the hierarchy of activities documented in the following sections. They grouped the processes within five general areas: **Management**, **Accessibility**, **Treatment**, **Pictures**, and **Protection**.

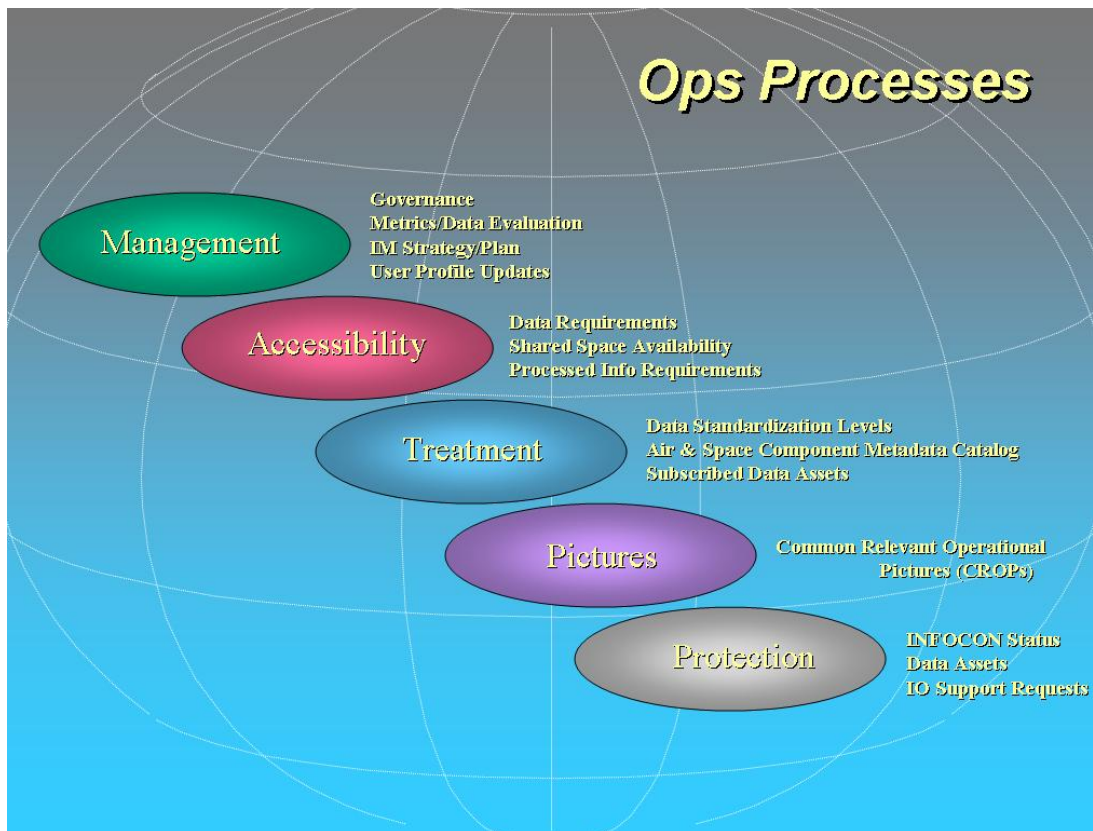


Figure 4-1: Key Ops Processes

4.1 Management – Provide Information Management/Net-Centricity Governance⁶

The DoD CIO, and counterparts at the theater, joint force and component levels establish a net-centric data governance process to promote and sustain successful data management practices across their domains. These net-centric governance processes also provide oversight of net-centric infrastructure development efforts. The JFACC IM Capability implements procedures to govern information management procedures within the Component. These should align with higher-level information management requirements and practices.

4.1.1 Provide Component Net-centric/Info Management Organization

The JFACC establishes an organization to manage the Component's IM capability. It comprises an Information Management Officer (IMO –Air), Information Management Board (IMB-Air), and Information Management Cell (IMC-Air).

4.1.1.1 Execute Information Management Officer (IMO-Air) Duties

The IMO-Air is the chief for all IM within the Component. The IMO-Air is responsible for coordinating with required external IMOs, IMBs, and other Components, as well as publishing the Component's Information Management Plan. The IMO-Air is intimately aware of the JFACC's information management requirements and possesses the authority to coordinate actions and processes to satisfy essential information needs. Under the supervision of the Chief of Staff (CoS), the IMO-Air works closely with higher HQ IMOs to ensure all required reports are up-channeled consistent with the battle rhythm. The IMO-Air serves as the focal point for information management issues with other functional component commander staffs. The IMO-Air also works closely with command administrative staffs and command and control elements (command posts) of all subordinate units in order to define reporting requirements and with Communication Support Team and communications/computer systems personnel to facilitate necessary information exchanges. The IMOs from the components or agencies under the JFC serve on the JIMB. The IMO-Air's duties include but are not limited to the following.

- *Direct Component Information Management Plan (IMP) Development.* The IMO-Air leads the effort to build the Component's IMP. The IMO-Air ensures the IMP aligns with the Joint IMP and all related Governances.
- *Manage Daily Battle Rhythm.* Utilizing the IMP, the IMO-Air ensures the Daily Battle Rhythm is maintained by monitoring daily operations requirements of higher

⁶ The following decomposed activities were developed using the *DoD Net-Centric Data Strategy* as a primary reference. Numerous activity descriptions are either derived from this reference or are reflected verbatim.

HQ via email, message traffic, web portals, or websites; ensuring all of the organizations' daily operations cycles meet the needs of the required commanders and organizations; and monitoring conflicting information management requirements.

- *Oversee Component Commander's Information Requirements (CCIR) Management.* CCIR is a prioritized list of information requirements identified by the JFACC that are critical to understanding the flow of the operation, identifying risks, and making timely decisions, and is a vital part of IM planning. The IMO-Air develops procedures to validate and manage CCIRs.
- *Oversee Request for Information (RFI) Management.* RFIs are vital means of requesting information to support military operations. The IMO-Air develops procedures to validate and manage RFIs.
- *Manage the IMC-Air.* The IMC-Air acts as the focal point for coordinating information within the organization and works directly for the IMO-Air. The IMO-Air ensures the IMC-Air carries out its assigned mission and responsibilities. The IMO-Air establishes the IMC-Air structure and appoints key management personnel.
- *Oversee IM Reports.* The IMO-Air establishes reporting requirements and timelines for subordinate units. The IMO-Air, through the IMC-Air, monitors unit reporting to ensure timeliness and correct formatting.
- *Chair the IMB-Air.* The IMO liaises directly with IMB chairpersons from Combined or Joint IMBs or other organizations' IMBs. The IMO-Air establishes the board agenda and presides over IMB-Air meetings.
- *Establish Data Standards to Ensure Data is Visible, Accessible, Understandable, Trusted, Interoperable, and Responsive.* Metrics are collected to track implementation and application of the approaches. The IMC-Air uses these metrics to evaluate data usage and the effectiveness of the overall Information Management Strategy. The IMO-Air establishes measurement techniques to ensure that metrics are captured in a useful and consistent manner and support higher-level metrics.

4.1.1.2 Manage Information Management Board (IMB-Air)

The IMB-Air is the venue used for coordinating information management within a specific component or agency. The IMB-Air is chaired by the IMO-Air and operates under the supervision of the JFACC, or other appropriate staff directorate, as determined by the JFACC. The IMB-Air comprises representatives from each staff section and supporting agency is used to actively resolve all internal, cross-functional, and JIMB-directed information management issues. The IMB-Air is the action arm of the IMO-Air and is responsible for the following.

- *Interface with Other Established IM Boards.* The IMB-Air is closely linked to other Component IMBs and the JIMB. The IMBs refer matters to one another for

resolution or guidance. The IMO-Air's designee will represent the Component as a member of other IMB's, as required.

- *Coordinate Component CCIRs.* The IMB-Air reviews CCIRs to ensure alignment with higher level CCIRs and the JFACC's critical information needs.
- *Manage Initial Shared Space Allocation.* The IMB-Air negotiates the initial Shared Space allocation for the JFACC. The IMB-Air processes Allocation Requests (ALLOREQ) and forwards the requests to the JIMB for approval or conflict resolution.
- *Manage RFI Issues.* The IMB-Air serves as an adjudication body to resolve RFI issues. An RFI that has been rejected or not satisfied within the organization may be brought before the IMB-Air for mediation.

4.1.1.3 Manage Information Management Cell (IMC-Air)

The IMC-Air acts as the internal focal point for coordinating IM within the organization. The Superintendent of the IMC-Air works closely with the IMO-Air to ensure IM policies and procedures are implemented and followed throughout their assigned areas. The IMC-Air is responsible for providing processes and business rules for life-cycle management of information as well as user assistance for common software applications, with responsibilities including but are not limited to:

- *Manage Workgroup Managers (WMs) (embedded/shared).* The IMC-Air provides oversight and training to WMs. WMs integrate information management with computer/network user management to effectively manage information as a corporate asset and strategic resource regardless of media.
- *Provide Overall Information-Related Administrative Support.* IMC-Air personnel carry out administrative duties to support the mission. This includes support for daily briefings, Director Read File, Significant Events Log, phone/e-mail listings, and managing the organization's portals, website, and homepage.
- *Manage Electronic File Plan (EFP).* The IMC-Air develops and maintains the EFP for the Component and ensures documentation is filed accordingly.
- *Manage Messaging Services.* The IMC-Air oversees message distribution within the Component.
- *Manage Suspense Control.* The IMC-Air monitors tasking within the organization and manages the Master Suspense Action Log.

4.1.2 Establish Component Commander's Information Requirements (CCIRs)

CCIRs are a vital part of JFACC IM Capability planning. CCIRs are a prioritized list of information requirements identified by the organizational commander that are critical to

understanding the flow of the operation, identifying risks, and making timely decisions. CCIRs are collated and reviewed for consistency and accuracy. The IMB-Air coordinates the initial set of CCIRs and additions as required. The validated CCIRs are forwarded to the JFACC for approval and authorization for release. To aid in updating and maintaining the prioritized list of CCIRs, information requirements are first organized and grouped within the following categories.

- *Establish Operational Environment Category CCIRs* – The JFACC requires information regarding the operational environment. This includes, but is not limited to, meteorological conditions; changes in national policy by the U.S., coalition, or neutral governments/forces; and relevant activities of non-governmental and private organizations.
- *Establish Friendly Force Category CCIRs* – The JFACC requires information pertaining to assigned forces in order to make timely and appropriate decisions. This category includes information regarding force locations, critical supply levels, and levels of force effectiveness.
- *Establish Threat Category CCIRs* – The JFACC requires information and intelligence to assist in assessing and understanding the situation. This category involves indications and warnings (I/W) of threat intents and future actions. Examples include information regarding force movements and changes in opposing force intents or policies.

4.1.3 Establish the JFACC IM Strategy and Plan

The JFACC IM Strategy and Plan describe the Component's approach to managing its net-centric information program and how it will support external organizations and higher-level information management programs.

The IM Strategy defines the role for information management within the Component and expands the focus to visibility and accessibility of data rather than just standardization. It also recognizes the need for data to be usable by unanticipated users and applications, as well as for those that have been predefined. Thus, the IM Strategy identifies the organizational approaches that will improve flexibility in data/information exchange and supports interoperability between systems.

The Component's Information Management Plan (IMP) documents the Component's IM construct, the Commander's (JFACC's) dissemination policy, information requirements and general procedures, digital rules of protocol, battle rhythm, and Continuity of Operations Plan (COOP). The IMC-Air assembles the key parts of IMP (detailed below) and submits the draft for IMO-Air coordination within the Component. The JFACC approves the final document. The IMP development process should include but is not limited to the following

- *Describe the IM Organization.* Based on higher level guidance, the IMC-Air provides the organizational construct to manage the Component's IM program. This includes key management roles, levels of authority, initial manpower requirements, sub-division structure, and operating locations.
- *Provide the Commander's Dissemination Policy (CDP).* The CDP serves as the JFACC's guidance portion of the IMP describing the dissemination of information within and outside of the component. It provides policy to guide information management decisions in the absence of specific guidance or detailed instructions. Critical information needs must be predetermined and prioritized to ensure support for critical missions, prevent overload of routine information, and provide guidance to apportion information assets.
- *Document Information Requirements/General Procedures.* The IMP documents basic information requirements (e.g., commander's CCIRs) and general procedures to manage information, data assets, and CROPs.
- *Document Digital Rules of Protocol.* The IMP establishes and documents the digital rules of protocol for the Component.
- *Document Commander's Battle Rhythm.* The IMP provides a general schedule of events for the organization's operations.
- *Include the Continuity of Operations Plan (COOP).* The COOP is an integral part of the IMP. The development process is documented in paragraph 4.5.1.

4.1.4 Establish Component Data Standards, Metrics, and Incentives

The IMO-Air establishes data standards to ensure data is visible, accessible, understandable, trusted, interoperable, and responsive. The IMC-Air collects metrics to track implementation and application of data and information. The IMC-Air develops measurement techniques to ensure that metrics are captured in a useful and consistent manner and support higher-level metrics.

4.1.5 Establish User Profile Standards

The IMC-Air establishes standardized user profiles for crew positions within the Component and key external positions. These profiles reflect user needs to address common operational requirements within the region. Workcenter Managers provide input from their respective areas. At the onset of operations, these profiles may require tailoring to meet operator needs.

4.2 Manage Information/Net-centric Data Accessibility

The IMC-Air processes information requirements. This may result in a new information product subscription, a data asset requirement, or a data asset subscription. New data asset requirements dictate an analysis of shared space availability.

4.2.1 Provide Data Access Services

Data access services are any mechanisms that help expose data that is not otherwise available to users and applications. For example, a data access service may be a registered, accessible software interface that allows users and applications to extract information from an inventory database. The IMC-Air should provide a list of available services to users and a list that documents all of the Component's data assets available for subscription.

4.2.2 Process Component Information Requirements

The IMC-Air receives and processes information requirements from users. Users may request: access to a net-centric data asset currently within a catalog; a modification to a cataloged data asset; establishment of a new (uncataloged) data asset; or a subscription to a net-centric data product (e.g., CROP – SIAP).

Once these requests/requirements are processed, they are rejected, accepted, referred, or returned for clarification. Acceptances are processed within the IMC-Air. Referrals are forwarded to applicable net-centric data/information product owners who may satisfy the request. Established or updated profiles may dictate user access to information products and data assets.

The IMC-Air processes Standardized User Profiles and Change Requests and submits product requests in the form of a CROP subscription, data asset subscription, or an RFI for unavailable data. The CROP subscription request is forwarded to the authority responsible for access to the required CROP. If approved, the request is processed and a subscription is established.

The IMO-Air oversees the Routine RFI process. RFIs are vital means of requesting information to support military operations. In a collaborative environment, a formal RFI should be submitted by exception only. This means the requestor should exhaust all available means of finding an answer before submitting an RFI. Once an RFI is submitted, the IMC-Air will determine its type, validity, and priority and analyze the availability of information.

- *Determine RFI Type (Operational/Intelligence).* There are two types of RFI: intelligence and operational. Intelligence RFIs are used to request information through intelligence infrastructure on enemy activities. These RFIs are ultimately used to also perform collection management and to ensure sensors and systems are collecting information to satisfy operational forces needs. On the other hand, operational RFIs are used to request information concerning friendly or coalition force statues, readiness information, etc. This information is used to support C2 functions, operational planning and other campaign management functions.
- *Determine RFI Validity.* The IMC-Air reviews the RFI to ensure it is properly formatted, references a CCIR, cites sources consulted for the RFI, and is stated as a specific, well-understood question.

- *Determine RFI Priority.* The IMC-Air assigns a priority to RFIs.
- *Determine Information/ Data Asset Availability.* The IMC-Air determines information/data sources to fulfill the RFI.
- *Compile RFI Analyses.* The IMC-Air assembles supporting analyses to fulfill the RFI. For RFIs that can not be satisfied, the IMC-Air prepares a Data Want Ad. A Data Want Ad will cue other IM organizations to search their catalogs for supporting information.

4.2.3 Manage Shared Space/Repositories

Virtual or actual shared spaces provide a “store and serve” mechanism for data assets or to accommodate changes to a cataloged data asset. The Joint Information Management Officer (IMO) allocates shared space to components within the Joint Force. The IMC-Air manages the JFACC’s allocated space and the repositories that make up that shared space. This shared space may be subdivided based on operational need. As discussed in the last Chapter, a sub-division forms an Operationally Accessible Shared Information Space (OASIS) and can be established for missions, functions, threads, etc of interest to the Component. The IMO-Air is responsible for allocating the Component’s shared space and granting access to required organizations so the data assets and IEPs can be available in a single, collaborative environment.

The IMC-Air monitors the repositories and shared space for capacity and data flow to ensure no issues arise and that the required information is available. If shared space is unavailable or insufficient, the IMO-Air through the IMB-Air requests an allocation adjustment from the JIMB.

Based on established guidance from the IMP and higher level organizations, the IMC-Air maintains an archive of the data/information. The Component’s data/information is archived as stipulated in the IMP. The IMC-Air maintains archives, provides status of the archival process, provides a back-up capability for the Component’s repositories, monitors status of that capability, and processes retrieval requests for archive information and data.

4.3 Treatment – Manage Organizational Net-Centric Data

Managing organizational net-centric data is the overarching process whereby the organization posts data assets and associated metadata, applies descriptors, establishes ontologies, maintains assigned catalogs, and registers metadata.

4.3.1 Define Component Ontologies

The IMC-Air establishes ontologies that best reflect the community understanding of the Component’s shared data. Ontologies include data categorization schemes, thesauruses, vocabularies, key word lists, and taxonomies. The ontologies are compiled and added to the Component’s Metadata Catalog. The following processes support ontology development:

- *Define Component Data Schemes:* The IMC-Air develops data categorization schemes.
- *Maintain Component Thesauruses:* The IMC-Air maintains thesauruses. Thesauruses identify related terms to assist translation services.
- *Maintain Component Key Word Lists:* The IMC-Air maintains key word lists for Component ontologies.
- *Define Component Taxonomies:* The IMC-Air defines taxonomies for Component taxonomies. These enhance discovery by providing a hierarchical means of searching for data. It affords users and applications with additional insight about data assets by indicating their placement among other data assets.
- *Maintain Component Vocabularies:* The IMC-Air maintains Component vocabularies that define terms used to describe data assets.

4.3.2 Identify Data Asset Requirements

The IMC-Air specifies descriptor requirements for the organization's data assets. This includes information regarding resource, summary content, security, and format descriptors.

- *Identify Authoritative Sources:* The IMC-Air identifies authoritative sources for key data assets in the Component's domain. The Component will publicize identified authoritative sources to the Enterprise, thus allowing users and applications to evaluate and understand the community- implied authority of data sources. The Component may have to resolve potentially conflicting sources and, where appropriate, coordinate with higher-level governance bodies to identify authoritative source(s).
- *Identify Security Requirements:* The IMC-Air establishes security requirements for each data asset. This includes disclosure and access guidelines, as well as data aggregation considerations. For example, an unclassified data asset may become classified when aggregated with other unclassified assets. The IMC-Air must also consider multinational access requirements.
- *Identify Shared Space Requirements:* The IMC-Air establishes requirements to accommodate shared space allocation to the Component and within the Component. Shared spaces (OASIS) will act as repositories where users and applications can submit, or post, data assets to the enterprise. The shared spaces will provide storage and serving mechanisms.
- *Identify Descriptor Requirements:* The IMC-Air specifies descriptor requirements for Component data assets. This includes information regarding resource, summary content, security, and format descriptors.

4.3.3 Associate Metadata with Data Asset

To facilitate discovery of data assets, users and applications provide discovery metadata in accordance with the DoD Discovery Metadata Standard (DDMS) for all data to be posted to shared spaces. The DDMS provides a common set of structured attributes that support discovery of data assets using search tools. The IMC-Air determines the desired level of discovery for a data asset (e.g., discovery of a database or a record within a database) or discovery of a document or a paragraph within a document. Metadata treatment of the data asset is compiled and forms the basis for the input to the metadata catalog and registry.

- *Apply Security Descriptor(s):* The IMC-Air applies security descriptor elements of the DDMS to allow security and privacy markings consistent with established standards where applicable. For Information Assurance (IA) and security, Global Information Grid Enterprise Services (GES) provide auditing tools that can track access, by individual user, of each data asset. GES may also provide access control to data assets based on security markings in the metadata.
- *Apply Resource Descriptor(s):* The IMC-Air applies resource descriptor elements of the DDMS to allow identification of the author, publisher, and sources contributing to the data, allowing users and applications to assess the derivation of the data (i.e., data pedigree). This metadata allows users and applications to select data from known sources. Reliable and quality sources will become more widely used, enhancing overall data quality throughout the enterprise as more data sources become visible.
- *Apply Summary Content Descriptor(s):* The IMC-Air applies summary content descriptor element set of the DDMS, thus providing (content-related) details about data assets. Content metadata provides topics, keywords, context, and other content-related information. It gives users and applications insight into the meaning and context of the data. Content metadata provides a basis for search engines to perform searches for data assets that address specific topics.
- *Apply Format Descriptor(s):* The IMC-Air applies the format descriptor element set of the DDMS. The format descriptors are useful when trying to understand the physical manifestation of an asset. In addition, the format descriptors contain optional information that describes the extent of the asset, such as file size, bit rate, and dimensions. Format-related metadata allows users and applications to narrow down information searches and to select products that meet their particular operating constraints.
- *Apply Extensible Layer:* To improve understanding, an extension of the discovery metadata standard is reserved for domain-specific or COI-specific metadata. This is represented as the extensible layer of the DDMS. With this extension layer, the IMC-Air is able to provide context relevant to their particular domain area and still be able to participate in enterprise-wide search and discovery. The IMC-Air registers

Component-specific content metadata requirements in the DoD Metadata Registry. These metadata requirements may then be integrated into appropriate enterprise and community services such as search and mediation.

4.3.4 Post Asset to Shared Space

Over time the JFACC IM Capability will migrate from maintaining private data (e.g., data kept within system-specific storage) to making data available in community- and enterprise-shared spaces (OASIS). The IMC-Air uses these shared spaces as repositories where users and applications can submit or post data assets to the enterprise. The shared spaces provide storage and serving mechanisms. Component data posted to shared spaces is advertised via the associated metadata and is discoverable with enterprise search tools.

4.3.5 Register Metadata

The DoD, Region and Joint Force registries contain metadata related to data structures, models, dictionaries, and schemas. These registries give developers and architects visibility into methods to compose and encode data and to share usage across the enterprise. Registration of the Component's metadata is critical to achieve the data goals of interoperability and understanding by promoting semantic and structural understanding.

4.3.6 Manage the Metadata Catalog

The IMC-Air uses the Component's metadata catalog to advertise the existence of shared data. The catalog contains information about all data assets contained in the associated shared space (including databases, system output files, web pages, documents, and access services). The Component's unique metadata elements for any data asset posted to a shared space are represented in the Component's metadata catalog. The IMC-Air establishes and maintains this catalog.

The catalog is searchable by applications or through user-friendly, web-based interfaces. The web-based interfaces should have a consistent look and feel and support posting of metadata to the catalog and data to the shared space. The catalog is searchable, either manually or automatically via agents, through application programming interfaces.

4.4 Manage Net-centric Pictures and Products

The IMC-Air builds and maintains standardized, Air & Space Component, net-centric subscription pictures; these are the Common Relevant Operational Pictures (CROPs) focused on key functional areas of the Component that are of interest to the joint force. The IMC-Air processes product requests to build new subscription products. They also monitor the status of all Component-subscribed CROPs.

4.4.1 Process Component CROP Development Request

The IMC-Air manages the dissemination and quality assurance of standardized net-centric subscription products, and processes requests for CROP development. This entails analyses

of operational needs, shared space requirements, and connectivity issues. If appropriate, the IMO-Air approves requests and provides guidance.

- *Analyze Operational Requirement.* The IMC-Air analyzes the CROP request for operational applicability. The requests may be returned for further justification, clarification or withdrawal.
- *Estimate Shared Space Requirement.* The IMC-Air analyzes the impact of the new CROP on the current allocation of shared space (OASIS). This requires an understanding of the data assets comprising the CROP, the anticipated users, and the amount of shared space available.
- *Estimate Connectivity Requirement.* Although primarily a communications function, the IMC-Air needs to understand who will require the new CROP and what types of communications systems and links are required to provide and receive it.
- *Approve Picture Development.* Based on justified operational need, an adequate amount of shared space and available communication systems and links, the IMO-Air will approve development of a new CROP. Disapprovals are forwarded to the requestor for reclamation as required. The IMO-Air provides CROP development guidance.

4.4.2 Develop Component CROP(s)

The IMC-Air manages CROP development. This entails data subscription, CROP formatting, shared space access, and CROP validation. If warranted, the IMO-Air approves the CROP for release.

- *Subscribe to Required Data:* The IMC-Air analyzes data asset requirements and establishes subscriptions to appropriate data assets.
- *Format Picture (Schema):* The IMC-Air works with the CROP requestor to build the picture, formatted to meet operational needs.
- *Access Shared Space:* Once formatted, the IMC-Air posts the picture to the Component's Shared Space; it is not accessible to the Component at this time.
- *Validate CROP:* The IMC-Air works with the requestor and experts from the operations community to ensure the proposed CROP meets operational needs. Security standards, to include access issues are addressed at this time. Once agreed, these standards are applied.
- *Approve CROP:* The validated CROP is turned over to IMO-Air who approves its release or returns it for further action.

4.4.3 Release and Monitor Component CROP(s)

The IMC-Air releases new CROPs to authorized subscribers. The IMC-Air monitors CROP implementation, produces a status report and notifies applicable personnel when problems occur.

4.5 Protection – Manage Component Information Assurance/Network Defense Operations

The JFACC Information Management Capability maintains the status of networks, preserves the integrity and availability of those networks, implements procedures to protect Component networks and communications means, and provides products to inform the computer network operations community of current computer network defense activities.

4.5.1 Manage Component INFOCON

With familiarity of INFOCON policy directives, IMC-Air develops management techniques that allow swift transition to varying levels of INFOCON. Activities supporting this process are as follows:

- *Identify Mission Critical, Support, & Admin Info Systems/Networks:* Effective INFOCON management commences with the IMC-Air identifying critical information nodes within the Component infrastructure. The types of IA protective measures, techniques and procedures needed for a system shall be determined based on information security and mission criticality.
- *Designate User Groups:* The IMC-Air develops a prioritized information systems position/user list. This list identifies users who require system access to perform mission essential duties on unclassified and classified networks. Those personnel who are key information processors are placed into an appropriate user group to support mission accomplishment. The IMO-Air designs user groups to limit access as much as feasible, and continue all operations with due regard to OPSEC and INFOSEC.
- *Develop Component Continuity of Operations Plan (COOP) Input:* The IMO-Air develops a Component COOP based upon actual mission requirements and information system capabilities. As an integral part of the Component's Information management Plan, the COOP may include: a list of critical information systems related to their respective mission; authorized users list, distinguished by tier groups; local INFOCON procedures; INFOCON quick reference matrix of critical systems; operational impact assessment of mission; and reporting instructions.
- *Manage INFOCON Change(s):* The IMC-Air notifies affected Component units about INFOCON changes. Notifications normally include the following information: date/time of report; current INFOCON; reason for declaration of this INFOCON; current/planned operation(s) or capabilities, units/organizations, networks, systems,

applications, or data assessed to be impacted or at risk; recommended or SECDEF-directed actions; references to relevant technical advisories, intelligence assessments, etc.; and POC contact information.

4.5.2 Support Information Assurance Vulnerability Alert (IAVA) Program

The IMC-Air acknowledges receipt of the IAVA, Information Assurance Vulnerability Bulletin (IAVB) or Information Assurance Vulnerability Technical Advisory. They take corrective action to comply with the IAV notification. They verify corrective action and report compliance. Compliance information shall include, at a minimum, the number of assets affected, the number of assets in compliance, and the number of assets with waivers.

4.5.3 Monitor Component Communications Links and Networks

The IMC-Air monitors the current operational status and availability of communications links and networks for the Component.

4.5.4 Manage Network Attack Impact Assessment

The IMO-Air, through the IMC-Air manages the Network Attack Impact Assessment for the Component. The Assessment is processed and submitted expediently to Joint IMO.

- *Identify Critical Information Systems Targeted:* Under the direction of the IMO-Air, the IMC-Air begins the assessment process by examining the critical information systems that are or may be affected by an impending attack.
- *List Missions/Operations Affected:* The IMC-Air lists missions or operations the Component is currently supporting, or projected to support in the near future, that may be affected by an attack.
- *Determine Technical Impact:* For each information system targeted, the IMC-Air determines the technical impact, i.e., to what degree the confidentiality, integrity, availability, authentication, and non-repudiation are affected. Additionally, they assess which critical applications and databases are impacted; how the technical impact of the malicious activity affects the Component's ability to execute its mission; how the impact on the component's ability to function affects support to current/projected operations. If no specific operations are ongoing or projected, the IMC-Air makes a determination of how general capability/readiness is affected.
- *Estimate Time and Resources Required to Restore Functionality:* For the technical impacts identified, IMC-Air estimates the time and resources required to restore functionality. They identify any interim workarounds.

5 Summary

The JFACC IM Capability Concept provides the operational basis for a JFACC Component to fully exploit the net-centric environment in 2010. This report presented the challenges, background factors, precepts, and key processes associated with this concept.

The net-centric environment of 2010 will be a demanding yet accommodating realm. It will invoke stringent management practices, new organizational designs, and innovative systems. With those in place, organizations will exploit net-centricity to optimize data/information flow, consistently produce decision quality information, and ultimately foment better decisions and more effective leadership.

References

A Guide for Communities of Interest (COIs) Implementing the DoD Net-Centric Data Strategy and the Air Force Information and Data Management Strategy, version 1, April 2005

Air Force Information and Data Management Strategy Policy, 3 March 2004

Air Force Information Strategy, Transformation through Information, August 2002

Department of Defense (DoD) Net-Centric Checklist, Version 2.1, 13 February 2004

Department of Defense (DoD) Net-Centric Data Strategy, 9 May 2003

Doctrinal Implications of the Standing Joint Force Headquarters (SJFHQ), Coordinating Draft, 20 April 2003

CENTAF Information Management Plan (IMP), Version 3.0, 2004

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001

Joint Task Force – Information Management (JTF-IM), Multi-Service Techniques, and Procedures for Joint Task Force Information Management (FM 6-02.85 (FM 101-4), (MCRP 3-40.2A), (NTTP 3-13.1.16), (AFTTP(I) 3-2.22), September 2003.

Military Transformation: A Strategic Approach, 2003

NCOW Reference Model, v0.9 25 June 2003

United States Air Force Transformation Flight Plan, 2004

Glossary

Communities of Interest (COIs) the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who, therefore must have shared vocabulary for the information they exchange. (*DoD Net-Centric Data Strategy*)

Component Commander's Information Requirements (CCIRs) a comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decision making process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements. (*CENTAF IMP*)

Data asset refers to any entity that is composed of data. For example, a database is a data asset that comprises data records. In this document, "data asset" means system or application output files, databases, documents, or web pages. "Data asset" also includes services that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., weather.com) would be a data asset. (*DoD Net-Centric Data Strategy*)

DoD Discovery Metadata Standard (DDMS) provides a common set of structured attributes that support the finding of data assets using search tools or other capabilities. The DDMS aids the discovery of data assets as a whole; hence, the discovery metadata in the DDMS will not always be required for individual records or elements. For example, the discovery metadata will always indicate the existence of a database containing certain kinds of information which may not identify the contents of specific database elements. The DDMS does not preclude the use of other metadata processes or standards. These tagging initiatives will only have to enhance their existing processes to include the DDMS for Enterprise discovery. (*DoD Net-Centric Data Strategy*)

Extensible Markup Language (XML) a tagging language used to describe and annotate data so it can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension. (*DoD Net-Centric Data Strategy*)

Global Information Grid (GIG) the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policymakers, and support personnel. (*DoD Net-Centric Data Strategy*)

Metadata descriptive information about the meaning of other data. Metadata can be provided in many forms, including XML. (*DoD Net-Centric Data Strategy*)

Metadata Catalog a system that contains the instances of metadata associated with individual data assets. Typically, a metadata catalog is a software application that uses a database to store and search records that describe such items as documents, images, and videos. Search portals and applications can use metadata catalogs to locate the data assets that are relevant to their queries. *(DoD Net-Centric Data Strategy)*

Metadata Registry a system that contains information that describes the structure, format, and definitions of data. Typically, a registry is a software application that uses a database to store and search data, document formats, definitions of data, and relationships among data. System developers and applications are the predominant users of a metadata registry. *(DoD Net-Centric Data Strategy)*

Net-centricity the realization of a networked environment (including infrastructure, systems, processes, and people) that enables a completely different approach to warfighting and business operations. *(DoD Net-Centric Data Strategy)*

Operationally Accessible Shared Information Space (OASIS) the established shared space bounded by specific operational needs that can be focused around missions, functions, threads, etc. An OASIS can be established for missions such as Close Air Support (CAS) or for operational threads that cut across missions, organizations or COIs.

Ontology includes data categorization schemes, thesauruses, vocabularies, key-word lists, and taxonomies. Ontologies promote semantic and syntactic understanding of data. *(DoD Net-Centric Data Strategy)*

Schema a diagrammatic representation, an outline, or a model. In relation to data management, a schema can represent any generic model or structure that deals with the organization, format, structure, or relationship of data. *(DoD Net-Centric Data Strategy)*

- Database table and relationship structure
- Document type definition (DTD)
- Data structure used to pass information between systems
- XML schema document (XSD) that represents a data structure and related information encoded as XML.

Schemas typically do not contain information specific to a particular instance of data. *(DoD Net-Centric Data Strategy)*

Shared space a mechanism that provides storage of and access to data for users within a bounded network space. Enterprise-shared space refers to a store of data that is accessible by all users within or across security domains on the GIG. A shared space provides virtual or physical access to any number of data assets (e.g., catalogs, web sites,

registries, document storage, and databases). As described in this Strategy, any user, system, or application that posts data uses shared space. *(DoD Net-Centric Data Strategy)*

Web services self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web services are consumable software services that typically include some combination of business logic and data. Web services can be aggregated to establish a larger workflow or business transaction. Inherently, the architectural components of web services support messaging, service descriptions, registries, and loosely coupled interoperability. *(DoD Net-Centric Data Strategy)*

User Profiles Standardized profiles for crew positions within the organization. These profiles should reflect user needs to address common operational requirements within the region. Workcenter Managers provide input from their respective areas. At the onset of operations, these profiles may be tailored to meet operator needs.

Acronyms

ACM	Airspace Control Measures
ACO	Airspace Control Order
AFC2ISRC	Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center
ALLOREQ	Allocation Request
ALSA	Air Land Sea Application
AOC WS	Air and Space Operations Center Weapon System
A/R	Air Refueling
ARCT	Air Refueling Control Time
ATO	Air Tasking Order
C2	Command and Control
C2C	Command and Control Constellation
CAOC	Combined Air and Space Operations Center
CAS	Close Air Support
CCIRs	Component Commander's Information Requirements
CDP	Commander's Dissemination Policy
CENTCOM	United States Central Command
CIO	Chief Information Officer
COI	Community of Interest
COOP	Continuity of Operations Plan
COP	Common Operational Picture
CoS	Chief of Staff
CROP	Common Relevant Operational Picture
DDMS	DoD Discovery Metadata Standard
DoD	Department of Defense
DQI	Decision Quality Information
EBO	Effects-based Operations
EFP	Electronic File Plan

EUCOM	European Command
FoS	Family of Systems
GES	Global Grid Enterprise Services
HQ	Headquarter
IA	Information Assurance
I/W	Indications and Warnings
IEP	Information Exchange Product
IM	Information Management
IMB	Information Management Board
IMC	Information Management Cell
IMO	Information Management Officer
IMB-A	Information Management Board – Air
IMC-A	Information Management Cell- Air
IMO-A	Information Management Officer- Air
IMP	Information Management Plan
INFOCON	Information Condition
INFOSEC	Information Security
IO	Information Operations
IAV	Information Assurance Vulnerability
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
JFACC	Joint Force Air and Space Component Commander
JFC	Joint Force Commander
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JFSOCC	Joint Force Special Operations Component Commander
JIMB	Joint Information Management Board
JTF	Joint Task Force
NAF	Numbered Air Force

OASIS	Operationally Accessible Shared Information Space
OPSEC	Operational Security
OV	Operational View
PACOM	Pacific Command
PBA	Predictive Battlespace Awareness
POC	Point of Contact
RFI	Request for Information
SECDEF	Secretary of Defense
TALCE	Tanker Airlift Control Element
TBMCS	Theater Battle Management Control System
TST	Time Sensitive Targeting
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
WM	Workgroup Manager
WOC	Wing Operations Center